各县（市、区）人民政府，市直属各单位：

《金华市公共数据授权运营实施细则（试行）》已经市政府同意，现印发给你们，请认真组织实施。

金华市人民政府办公室

2024 年 1 月 12 日

金华市公共数据授权运营实施细则（试行）

为规范公共数据授权运营管理，加快公共数据有序开发利用，培育数据要素市场，激活经济发展新动能，推动数字经济高质量发展，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》《浙江省公共数据条例》《浙江省公共数据授权运营管理办法（试行）》等有关法律法规和文件规定，结合本市实际，制定本细则。

一、总则

（一）总体要求。

公共数据授权运营坚持中国共产党的领导，遵循依法合规、安全可控、统筹规划、稳慎有序的原则，按照“原始数据不出域、数据可用不可见”的要求，在保护个人信息、商业秘密、保密商务信息和确保公共安全的前提下，向社会提供数据产品和服务。优先面向与民生紧密相关、行业增值潜力显著、产业战略意义重大的领域开展授权运营。禁止开放的公共数据不得授权运营。

（二）适用范围。

本细则适用于本市行政区域内与公共数据授权运营相关的数据活动。

（三）名词定义。

公共数据授权运营，是指县级以上政府按程序依法授权法人或者非法人组织（以下统称“授权运营单位”），对授权的公共数据进行加工处理，开发形成数据产品和服务，并向社会提供的行为。

授权运营域，是指由公共数据主管部门依托一体化智能化公共数据平台组织建设和运维的，为授权运营单位提供加工处理授权运营公共数据服务的特定安全域，具备安全脱敏、访问控制、算法建模、监管溯源、接口生成、封存销毁等功能。

授权运营协议，是指县级以上政府与授权运营单位就公共数据授权运营达成的书面协议，明确双方权利义务、授权运营范围、运营期限、合理收益的测算方法、数据安全要求、期限届满后资产处置、退出机制和违约责任等。

数据产品和服务，是指利用公共数据加工形成的数据包、数据模型、数据接口、数据服务、数据报告、业务服务等。

（四）授权方式。

授权运营坚持“总量控制、因地制宜、公平竞争”原则，按照应用场景开展授权运营。应用场景应具有重大经济价值或社会价值，具有较强的可实施性，在授权运营期限内有明确目标和计划，能够取得显著成效。场景所需公共数据需求应当符合最小必要的原则。

（五）定价及收益分配。

探索建立公共数据定价管理和收益分配机制，探索将公共数据授权运营纳入政府国有资源（资产）有偿使用范围，结合具体应用场景确定公共数据使用定价

和收益分配方式。推动用于公共治理、公益事业的公共数据有条件无偿使用，探索用于产业发展、行业发展的公共数据有条件有偿使用。

（六）公共数据开放激励。

公共数据主管部门应探索建立公共数据开放激励机制，对公共管理和服务机构的数据开放数量、授权数量、数据质量等方面进行数据贡献情况评估，评估结果作为部门信息化项目绩效的重要参考。

二、职责分工

（一）建立公共数据授权运营管理工作协调机制，由公共数据主管部门会同网信、发改、经信、公安、国家安全、司法行政、财政、市场监管等部门负责本市行政区域内授权运营工作的统筹管理、安全监管和监督评价，建立健全公共数据授权运营相关制度规范和工作机制；确定授权运营领域；监督指导公共数据授权运营评估工作；负责审议给予授权、终止或撤销授权等重大事项，协调解决公共数据授权运营工作中遇到的重大问题；负责组建公共数据授权运营工作专家组。

（二）公共数据主管部门负责公共数据授权运营具体实施工作，指导、协调、督促其他有关部门按照各自职责做好授权运营相关工作，负责授权运营域的建设和运维，并负责会同相关领域主管部门研究确定领域具体安全要求。市、县（市、区）政府设置公共数据授权运营合同专用章，由公共数据主管部门管理使用。

（三）公共数据授权运营工作专家组负责对公共数据授权运营申请单位资质、场景可行性、数据需求清单合理性、数据产品和服务合规性等进行技术评审，就授权运营工作的规范性、先进性、科学性等方面提出针对性优化意见建议，为授权运营工作的组织、运行、决策提供咨询意见和决策支撑。

（四）发改、经信、财政、市场监管等部门按照各自职责，做好数据产品和服务流通交易的监督管理工作。

（五）网信、保密、密码管理、公安、国家安全等部门按照各自职责，做好授权运营的安全监管工作。

（六）公共管理和服务机构负责做好本领域公共数据的治理、申请审核及安全监管等授权运营相关工作。

三、授权程序

（一）信息发布。

公共数据主管部门发布重点领域开展授权运营的通告，明确申报条件。

（二）申请提交。

授权运营申请单位应遵循《浙江省公共数据授权运营管理办法（试行）》关于授权运营单位安全条件的基本安全要求、技术安全要求、应用场景安全要求和重点领域具体安全要求，在规定时间内，向公共数据主管部门提出需求，并提交授权运营申请表、最近 1 年的第三方审计报告和财务会计报告、数据安全承诺书、安全风险自评报告等材料。

（三）资格审查。

1.材料预审。公共数据主管部门对授权运营申请单位的申报材料进行初步审查，申请单位提交材料不齐全或者不符合形式要求的，应在规定时间内补齐。

2.专家评审。公共数据主管部门会同相关单位组织召开专家评审会，对授权运营中的业务和技术问题进行论证，出具评审意见。

3.资格终审。公共数据主管部门根据评审意见召开协调机制会议拟定授权运营单位，提交本级政府确定。

（四）上报备案。

公共数据主管部门应及时将审定后的授权运营单位与应用场景向省政府备案。

（五）社会公开。

公共数据主管部门及时向社会公开授权运营单位、授权运营场景等相关信息。

（六）协议签订。

本级政府与授权运营单位签订授权运营协议。授权运营协议期限一般不超过1年，期限届满后，授权运营单位可按程序重新申请。

（七）授权终止。

当授权运营协议终止或撤销时，公共数据主管部门应及时关闭授权运营单位的授权运营域使用权限，删除授权运营域内留存的相关数据，并按照规定留存相关网络日志不少于6个月。

四、授权运营行为规范

授权运营单位应根据授权运营范围，依法依规进行公共数据申请、加工、运营。在开展授权运营过程中，因数据汇聚、关联分析等原因发现数据间隐含关系与规律，并危害国家安全、公共利益，或侵犯个人信息、商业秘密、保密商务信息的，应立即停止相应的数据处理活动，及时向公共数据主管部门报告数据风险情况。

（一）数据申请获取。

授权运营单位应通过授权运营域提交公共数据需求申请，公共数据主管部门会同相关公共管理和服务机构审核确认后，将相应公共数据资源纳入授权运营域统一管理，并向授权运营单位开放相应权限。授权运营单位相关管理、技术人员

须经实名认证、备案与审查，签订保密协议，通过授权运营岗前培训后，方可开通授权运营域的权限。

涉及个人信息、商业秘密、保密商务信息的公共数据，应经过脱敏、脱密处理，或经相关数据所指向的特定自然人、法人、非法人组织依法授权同意后获取。涉及社会数据时，经公共数据主管部门审核批准后，授权运营单位可将依法合规获取的社会数据导入授权运营域，与授权运营的公共数据进行融合计算。

（二）数据加工处理。

授权运营单位应在授权运营域内对公共数据进行加工处理形成数据产品，数据加工人员使用经抽样、脱敏后的公共数据进行数据产品的模型训练与验证。授权运营单位在数据加工处理或提供服务过程中发现公共数据质量问题的，可以向公共数据主管部门提出数据治理需求。需求合理的，公共数据主管部门应督促数据提供单位在规定期限内完成数据治理。

（三）产品形成。

授权运营单位加工形成的数据产品和服务接受公共数据主管部门审核后上线。原始数据或者通过可逆模型或算法还原出原始数据的数据产品和服务，不得导出授权运营域。经公共数据主管部门审核批准后导出授权运营域的数据产品和服务，不得用于或变相用于未经审批的应用场景。

（四）产品运营。

授权运营单位应坚持依法合规、普惠公平、收益合理的原则，确定数据产品和服务的价格。授权运营单位在运营期限内，应当向公共数据主管部门提交授权运营年度运营报告，报告应当包括本单位与授权运营相关的数据产品和服务存储、

加工处理、分析利用、安全管理及市场运营情况等内容。数据产品和服务应当按照国家、省和市有关数据要素市场规则流通交易。

（五）第三方管理。

授权运营单位应加强对合作方、第三方机构及相关人员管理，保障公共数据产品和服务合法合规安全应用，防范违规使用、转卖、泄露或其他不当应用情况。授权运营单位发现上述情况的，应该采取相关措施避免损失扩大，并上报公共数据主管部门。

五、授权运营域

（一）建设原则。

市公共数据主管部门应按照全省授权运营域建设标准，依托一体化智能化公共数据平台建设授权运营域。全市公共管理和服务机构、县（市、区）依托市级授权运营域开展授权运营工作。

（二）系统功能。

授权运营域应实现网络隔离、租户隔离、开发与生产环境隔离，具备数据脱敏处理、数据产品和服务审核、数据加工处理人员的实名认证与备案管理等功能，满足政府监管需求，支持集成外部数据，具备分布式隐私计算能力，满足授权运营单位的基本数据加工需求。

（三）系统运维。

市公共数据主管部门应当加强技术投入和运维管理，制定相关管理规范和技术标准，确保授权运营域安全稳定运行。

六、数据安全

（一）公共数据授权运营坚持统筹发展和安全的原则，按照“公共数据分类分级”要求，加强公共数据全生命周期安全和合法利用管理，确保数据来源可溯、去向可查、行为留痕、责任可究。

（二）公共数据主管部门应根据《浙江省公共数据授权运营管理办法（试行）》相关要求，加强数据安全管理。应建立授权运营域安全管理制度，健全安全保障措施，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入、数据泄露等危害网络及数据安全的风险。定期组织授权运营单位开展安全培训、应急演练和攻防演练。

（三）公共数据主管部门应会同网信、保密、密码管理、公安、国家安全等单位，按照“一授权一预案”要求，结合授权运营的应用场景制定应急预案，并组织应急演练。未制定应急预案的，不得开展授权运营工作。

发生数据安全事件时，公共数据主管部门应按照应急预案启动应急响应，采取相应的应急处置措施，防止危害扩大，消除安全隐患。

（四）公共数据授权运营安全坚持“谁运营谁负责、谁使用谁负责”的原则。授权运营单位主要负责人是运营公共数据安全的第一责任人。授权运营单位应建立健全高效的技术防护和运行管理体系，完善安全制度，确保公共数据安全，切实保护个人信息。

（五）授权运营单位应制定授权运营安全应急处置预案并组织应急演练，加强防攻击、防泄露、防窃取的监测、预警、控制和应急处置能力建设。

七、监督管理

（一）建立健全监督机制，加强对授权运营域、数据产品和服务、数据管理等安全合规情况的监督检查，并督促整改落实。公共数据主管部门应会同有关部

门或委托第三方机构组织对授权运营单位开展授权运营和安全评估。对授权运营单位实行动态管理，评估结果作为再次申请授权运营的重要依据。

（二）市场监管部门协同发改、经信、财政等单位完善数据产品和服务的市场化运营管理制度。对违反反垄断、反不正当竞争、消费者权益保护等法律法规规定的，由有关单位按照职责依法处置，相关不良信息依法记入其信用档案。

（三）知识产权主管部门会同发改、经信、司法行政等单位建立数据知识产权保护制度，推进数据知识产权保护和运用。

（四）授权运营单位违反授权运营协议的，公共数据主管部门应按照协议约定要求其改正，并暂时关闭其授权运营域使用权限。授权运营单位应在约定期限内改正，并反馈改正情况；未按要求完成改正的，终止其相关公共数据的授权。

（五）授权运营单位存在违反网络安全、数据安全、个人信息保护有关法律法规规定行为的，由网信、公安等单位按照职责依法予以查处，相关不良信息依法记入其信用档案。

八、附则

本细则自 2024 年 2 月 15 日起施行。国家和省对公共数据授权运营管理另有规定的，从其规定。